„HP Sure Admin“ naudotojo vadovas

SUVESTINĖ

„HP Sure Admin“ leidžia IT administratoriams saugiai valdyti slaptus įrenginių programinės aparatinės įrangos nustatymus, vietoj slaptažodžio naudojant sertifikatus ir šifravimą viešuoju raktu, tiek tvarkant nuotoliniu būdu, tiek vietoje.

Juridinė informacija

„Apple“ yra „Apple Computer, Inc.“ prekių ženklas, įregistruotas JAV ir kitose šalyse.

„Google Play“ yra „Google LLC“ prekių ženklas.

Konfidenciali kompiuterių programinė įranga. Norint turėti, naudotis arba kopijuoti reikalinga galiojanti HP licencija. Dera su FAR 12.211 ir 12.212; komercinė kompiuterių programinė įranga, kompiuterių programinės įrangos dokumentacija ir komercinių prekių techniniai duomenys JAV vyriausybei licencijuojami pagal gamintojo standartinę komercinę licenciją.

Šiame dokumente pateikta informacija gali būti pakeista apie tai iš anksto neįspėjus. HP gaminiams ir paslaugoms taikomos garantijos nustatytos su tais gaminiais ir paslaugomis pateikiamuose raštiškuose garantijos dokumentuose. Jokie šiame dokumente esantys teiginiai negali būti laikomi papildoma garantija. HP neprisiima atsakomybės už galimas technines ir redagavimo klaidas ar praleidimus šiame dokumente.

Antrasis leidimas: 2021 m. spalio mėn.

Pirmasis leidimas: 2019 m. gruodžio mėn.

Dokumento numeris: L83995-E22

Turinys

1 Darbo pradžia

„HP Sure Admin“ leidžia IT administratoriams saugiai valdyti slaptus įrenginių programinės aparatinės įrangos nustatymus, vietoj slaptažodžio naudojant sertifikatus ir šifravimą viešuoju raktu, tiek tvarkant nuotoliniu būdu, tiek vietoje.

„HP Sure Admin“ sudaro šios dalys:

- **Paskirties kompiuteris.** Valdomos platformos, kurios palaiko patobulintą BIOS autentifikavimo režimą.
- **HP Manageability Integration Kit (MIK).** „System Center Configuration Manager“ (SCCM) arba HP „BIOS Configuration Utility“ (BCU) papildinys nuotoliniam BIOS nustatymų valdymui.
- **„HP Sure Admin“ Local Access Authenticator.** Slaptažodį pakeičianti telefono programa, įgalinanti vietinę prieigą prie BIOS sąrankos nuskaitant QR kodą, kad būtų gautas vienkartinis PIN.

„HP Sure Admin“ naudojimas

Šiame skyriuje aprašyta, kaip naudoti „HP Sure Admin“.

1. Atidarykite „HP Sure Admin“ papildinį naudodami „HP Manageability Integration Kit“ (MIK) papildinį skirtą „System Center Configuration Manager“ (SCCM) arba patobulintai „BIOS Configuration Utility“ (BCU).
2. Atsisiųskite „HP Sure Admin“ telefono programą iš „Google Play™“ arba iš „Apple App Store®“ parduotuvės.
3. Sukurkite paskirties įrenginio ir „HP Sure Admin“ telefono programos naudojamą raktų porą, kad gautumėte vienkartinį PIN ir galėtumėte atrakinti BIOS.

„HP Sure Admin“ išjungimas

Šiame skyriuje pateikiamos „HP Sure Admin“ išjungimo parinktys.

- BIOS F10 nustatyme pasirinkite **Atkurti numatytuosius gamyklinius saugos nustatymus**.

PASTABA: Turite būti vietoje ir pateikti autentifikavimo PIN naudodamiesi „HP Sure Admin“ telefono programa, kad gautumėte prieigą prie F10 nustatymų.

- Naudokite BCU komandą, kad nuotoliniu būdu paskambintumėte WMI **Atkurti numatytuosius gamyklinius saugos nustatymus**.

PASTABA: Jei reikia daugiau informacijos, žr. „HP BIOS Configuration Utility“ (BCU) naudotojo vadovą.

- VIK saugos užtikrinimo puslapyje pasirinkite **Nepateikimas**.

2 Raktų kūrimas ir valdymas

Atlikite VIK saugos užtikrinimą ir tik tada įjunkite patobulintą BIOS autentifikavimo režimą. Jei norite kurti ir eksportuoti raktus, turi būti įjungtas patobulintas BIOS autentifikavimo režimas. BIOS autentifikavimo režimo įjungimas:

▲ atidarykite „HP Sure Admin“ papildinį ir pasirinkite **Patobulintas BIOS autentifikavimo režimas**, kad galėtumėte kurti ir eksportuoti raktus.

Raktų kūrimas ir eksportavimas

Sukurti vietinės prieigos raktų poras ir įjungti „HP Sure Admin“ telefono programą, kad pasiektumėte raktą, galite 3 skirtingais būdais.

- Rakto sukūrimas ir eksportavimas rankiniu būdu 2 puslapyje
- Rakto sukūrimas ir eksportavimas naudojant „Azure AD“ atšaukimą 3 puslapyje
- Rakto sukūrimas ir išsiuntimas į „Azure AD“ grupės „OneDrive“ 3 puslapyje

Rakto sukūrimas ir eksportavimas rankiniu būdu

pasinaudokite šia parinktimi ir eksportuokite vietinį prieigos patvirtinimo raktą, tada rankiniu būdu paskirstykite jį „HP Sure Admin“ telefono programai naudodamiesi el. paštu arba kitu būdu.

PASTABA: Šiai parinkčiai nebūtina, kad „HP Sure Admin“ telefono programa turėtų prieigą prie interneto, kad gautų vienkartinį PIN.

1. Laukelyje **Rakto pavadinimas** suteikite savo raktui pavadinimą.
2. Laukelyje **Prieigos slaptažodis** įveskite prieigos slaptažodį.

   PASTABA: Prieigos slaptažodis naudojamas apsaugant eksportuotą raktą ir turi būti pateiktas, kad „HP Sure Admin“ telefono programos naudotojas galėtų importuoti raktą.

3. Pasirinkite **Naršyti** ir pasirinkite, kur bus eksportuojamas kelias sistemoje.
4. Pasirinkite **Kurti raktą**. Jūsų raktas bus sėkmingai sukurtas, kai prie mygtuko **Kurti raktą** parodomas pranešimas **Raktas sėkmingai sukurtas**.
5. Pasirinkite **Kitas**. Suvestinės puslapyje rodomi jūsų įvesti „HP Sure Admin“ nustatymai.
6. Pasirinkite **Išsaugoti strategiją**. Strategija yra išsaugota, kai parodomas pranešimas **Išsaugota sėkmingai**.
7. Eikite į aplanką, kuriame išsaugojote raktą ir paskirstykite jį „HP Sure Admin“ telefono programos naudotojui panaudodami tam naudotojo įrenginiui prieinamą būdą, pvz., el. paštą. Šiam naudotojui reikės prieigos slaptažodžio, kad galėtų importuoti raktą. HP rekomenduoja naudoti skirtingus rakto ir prieigos slaptažodžio paskirstymo mechanizmus.

   PASTABA: Jei siunčiate QR kodą, siųskite jį pradinio dydžio. Programa negali teisingai nuskaityti paveikslėlio, jei jis mažesnis nei 800 × 600.

Rakto sukūrimas ir eksportavimas naudojant „Azure AD“ atšaukimą

Naudokite šią parinktį, jei norite prijungti vietinės prieigos raktą prie nurodytos „Azure Active Directory“ grupės, ir nurodykite, kad prieš pateikiant vietinės prieigos PIN „HP Sure Admin“ telefono programa reikalautų patvirtinti naudotoją „Azure Active Directory“ ir patvirtinti, kad naudotojas yra nurodytos grupės narys. Naudojant šį būdą taikomas rankinis vietinio prieigos patvirtinimo rakto platinimas telefono programai el. paštu arba kitu būdu.

PASTABA: Šiai parinkčiai būtina, kad „HP Sure Admin“ telefono programa turėtų prieigą prie interneto, kad gautų vienkartinį PIN.

1. Laukelyje **Rakto pavadinimas** suteikite savo raktui pavadinimą.
2. Laukelyje **Prieigos slaptažodis** įveskite prieigos slaptažodį.

   PASTABA: Prieigos slaptažodis naudojamas apsaugant eksportuotą raktą ir turi būti pateiktas, kad „HP Sure Admin“ telefono programos naudotojas galėtų importuoti raktą.

3. Pasirinkite **„Azure AD“ prisijungimas** ir prisijunkite.
4. Išskleidžiamajame laukelyje **„Azure AD“ grupės pavadinimas** pasirinkite savo grupės pavadinimą. Jei norite gauti prieigą prie rakto, turite būti grupės nariu.
5. Pasirinkite **Naršyti** ir pasirinkite, kur bus eksportuojamas kelias sistemoje.
6. Pasirinkite **Kurti raktą**. Jūsų raktas bus sėkmingai sukurtas, kai prie mygtuko **Kurti raktą** parodomas pranešimas **Raktas sėkmingai sukurtas**.
7. Pasirinkite **Kitas**. Suvestinės puslapyje rodomi jūsų įvesti „HP Sure Admin“ nustatymai.
8. Pasirinkite **Išsaugoti strategiją**. Strategija yra išsaugota, kai parodomas pranešimas **Išsaugota sėkmingai**.
9. Eikite į aplanką, kuriame išsaugojote raktą ir paskirstykite jį „HP Sure Admin“ telefono programos naudotojui panaudodami tam naudotojo įrenginiui prieinamą būdą, pvz., el. paštą. Šiam naudotojui reikės prieigos slaptažodžio, kad galėtų importuoti raktą. HP rekomenduoja naudoti skirtingus rakto ir prieigos slaptažodžio paskirstymo mechanizmus.

   PASTABA: Jei siunčiate QR kodą, siųskite jį pradinio dydžio. Programa negali teisingai nuskaityti paveikslėlio, jei jis mažesnis nei 800 × 600.

Rakto sukūrimas ir išsiuntimas į „Azure AD“ grupės „OneDrive“

(Rekomenduojama) Naudokite šią parinktį, kad telefone nebūtų saugomas vietinis prieigos patvirtinimo raktas. Kai pasirenkate šią parinktį, VIK vietinį prieigos patvirtinimo raktą išsaugo nurodytame „OneDrive“ aplanke, kurį gali pasiekti tik įgaliota grupė. „HP Sure Admin“ telefono programos naudotojas bus paragintas patvirtinti naudojant „Azure AD“ kiekvieną kartą, kai bus reikalingas PIN.

1. Laukelyje **Rakto pavadinimas** suteikite savo raktui pavadinimą.
2. Laukelyje **Prieigos slaptažodis** įveskite prieigos slaptažodį.
3. Pasirinkite **„Azure AD“ prisijungimas** ir prisijunkite.
4. Išskleidžiamajame laukelyje „Azure AD“ grupės pavadinimas pasirinkite savo grupės pavadinimą.

   PASTABA: Jei norite gauti prieigą prie rakto, turite būti grupės nariu.

5. Laukelyje **„OneDrive“** įveskite to „OneDrive“ aplanko pavadinimą, kuriame norite išsaugoti raktą.
6. Pasirinkite **Naršyti** ir pasirinkite, kur bus eksportuojamas kelias sistemoje.
7. Pasirinkite **Kurti raktą**.

PASTABA: Jūsų raktas bus sėkmingai įtrauktas į nurodytą „OneDrive“ aplanką ir eksportuotas į nurodytą vietinį aplanką, kai prie mygtuko **Kurti raktą** nus parodyta piktograma su pranešimu **Raktas sėkmingai sukurtas**.

8. Pasirinkite **Kitas**. Suvestinės puslapyje rodomi jūsų įvesti „HP Sure Admin“ nustatymai.
9. Pasirinkite **Išsaugoti strategiją**. Strategija yra išsaugota, kai parodomas pranešimas **Išsaugota sėkmingai**.

PASTABA: Šioje situacijoje nereikia nieko siųsti į „HP Sure Admin“ telefono programą, kad ji būtų iš anksto paruošta. Paskirties kompiuteriai yra iš anksto paruošti nurodyti „OneDrive“ vietą, kuri įtraukiama į QR kodą. „HP Sure Admin“ telefono programa naudoja šį žymeklį, kad pasektų „OneDrive“ vietą, jei naudotojas yra įgaliotos grupės narys ir sėkmingai patvirtina tapatybę.

3 Telefono sąranka

Atsisiųskite „HP Sure Admin“ telefono programą iš „Google Play“ arba iš „Apple Store“ parduotuvės.

- „Android“ telefonuose atsisiųskite „HP Sure Admin“ iš „Google“ parduotuvės.
- „iOS“ telefonuose atsisiųskite „HP Sure Admin“ iš „Apple Store“ parduotuvės.

„HP Sure Admin“ telefono programos naudojimas atrakinant BIOS

„HP Sure Admin“ mobiliesiems įrenginiams skirta programa pakeičia BIOS slaptažodžio naudojimą vietinei prieigai prie BIOS sąrankos pateikiant vienkartinį PIN, kuris gaunamas nuskaičius QR kodą, kurį pateikia paskirties kompiuteris.

Atlikite toliau nurodytus veiksmus, jei raktą norite įrašyti telefone, kai jis atsiunčiamas telefono programos naudotojui. Toliau pateiktame pavyzdyje raktas yra el. paštu išsiųstas „HP Sure Admin“ telefono programos naudotojui, ir naudotojas atidaro el. paštą savo telefone.

1. Atidarykite el. laišką, kuriame yra raktas.
2. Kai parodomas puslapis **Registracija**, laukelyje **Įveskite prieigos slaptažodį** įveskite prieigos slaptažodį, o laukelyje **Įveskite el. pašto adresą** įveskite el. pašto adresą, kad raktas būtų iššifruotas ir pridėtas prie „HP Sure Admin“ programos. Atrakinimo PIN numeris rodomas puslapyje **Jūsų PIN**.

   PASTABA: Atlikus šį veiksmą raktas išsaugomas mobiliajame įrenginyje ir užbaigiama registracija. Dabar galite naudoti „HP Sure Admin“ telefono programą, kad pasiektumėte bet kurį įrenginį, kuris yra nustatytas pasiekti naudojantis šiuo raktu. El. pašto adresas būtinas, tik jei to reikalauja administratorius.

3. BIOS laukelyje **Įveskite atsakymo kodą** įveskite PIN.

Prieigos prie BIOS sąrankos gavimas po registracijos

Jei norite gauti prieigą prie BIOS sąrankos paskirties kompiuteryje, po registracijos atlikite toliau nurodytus veiksmus.

1. Paskirties kompiuterio paleisties metu eikite į BIOS sąranką.
2. Telefono programoje pasirinkite **Nuskaityti QR kodą** ir nuskaitykite paskirties kompiuteryje pateikiamą QR kodą.
3. Jei būsite paraginti patvirtinti naudotojo tapatybę, pateikite savo kredencialus.
4. Atrakinimo PIN numeris rodomas puslapyje **Jūsų PIN**.
5. Įveskite PIN paskirties kompiuterio BIOS laukelyje **Įveskite atsakymo kodą**.

BIOS atrakinimas naudojant „Azure AD“ grupės „OneDrive“

Atlikite toliau nurodytus veiksmus, jei norite naudoti „HP Sure Admin“, kad atrakintumėte BIOS su „Azure AD Group OneDrive“.

1. Pasirinkite **Nuskaityti QR kodą** ir nuskaitykite BIOS QR kodą.

PASTABA: „HP Sure Admin“ programa parodo „Azure AD“ prisijungimo puslapį.

2. Prisijunkite prie „Azure“ paskyros.
3. BIOS laukelyje **Įveskite atsakymo kodą** įveskite PIN.

PASTABA: Šiuo atveju „HP Sure Admin“ programa rakto neišsaugo. „HP Sure Admin“ telefono programa turi turėti prieigą prie tinklo ir naudotojas turi būti patvirtintas kiekvieną kartą, kai reikia vienkartinio PIN.

4 „HP Sure Admin“ klaidų kodai

„HP Sure Admin“ ir KMS administratoriaus konsolės klaidų kodus, tipus ir jų aprašus rasite šiame skyriuje pateikiamoje lentelėje.

4-1 lentelė „HP Sure Admin“ programos klaidų kodai, tipai ir jų aprašai

Klaidos kodas	Klaidos tipas	Aprašas
100	QRCodeUnknownError	Bendroji klaida.
101	QRCodeDeserialization	Nepavyksta nuskaityti QR kodo JSON failo. Eilutės nėra nurodytame JSON faile arba duomenys yra netinkami.
102	QRCodeInvalidImage	Nuskaitytas QR kodo paveikslėlis yra netinkamas. Neįmanoma nuskaityti QR kodo paveikslėlio failo.
103	QRCodeNoPayload	Nuskaitytas QR kodo paveikslėlis yra netinkamas. Paveikslėlio failas neturi JSON perdavimo.
104	QRCodeInvalid	Neįmanoma nuskaityti QR kodo JSON failo. Eilutės nėra nurodytame JSON faile arba QR paveikslėlio duomenys yra netinkami.
105	QRCodeInvalidKeyIdHash	Viešojo rakto maiša QR kodo JSON faile neatitinka registracijos paketo viešojo rakto maišos („KeyID“ duomenys).
106	QRCodeTampered	Nuskaitytas QR kodo paveikslėlis yra sugadintas ir netinkamas.
107	QRCodeTamperedOrInvalidPassPhrase	Nuskaitytas QR kodo paveikslėlis yra sugadintas ir netinkamas arba įvestas prieigos slaptažodis yra neteisingas.

4-2 lentelė „OneTime“ prieigos raktas iš „OneDrive“ klaidų, tipų ir jų aprašų

Klaidos kodas	Klaidos tipas	Aprašas
200	OneTimeKeyError	Bendroji klaida.
201	OneTimeKeyNoUserGroups	Prisiregistravęs naudotojas nepriklauso jokiai jūsų organizacijos AD grupei.
203	OneTimeKeyInvalidUserGroup	Prisiregistravęs naudotojas nepriklauso jokiai AD grupei, kuriai yra priskirtas šis rakstas.
204	OneTimeKeyQRFileDoesNotExist	„OneTime“ rakto failo nėra AD grupės „OneDrive“ aplanke.
205	OneTimeKeyInvalidQRFile	„OneTime“ rakto failas AD grupės „OneDrive“ aplanke yra netinkamas.
206	OneTimeKeyInvalidQRpayload	„OneTime“ rakto failas yra, bet negali nuskaityti failo perdavimo.

4-3 lentelė „Azure AD“ įgaliojimo klaidos

Klaidos kodas	Klaidos tipas	Aprašas
300	AzureADUnknownError	Bendroji klaida.
301	AzureADInvalidDomain	El. pašto adresas neatitinka domeno pavadinimo, kuris nurodytas QR kodo paveikslėlyje.
302	AzureADAccessToken	Įsigyjant prieigos raktą iš „Azure AD“ įvyko klaida. Naudotojas negali prisijungi prie organizacijos „Azure AD“, arba programa neturi reikiamų leidimų, kad prijungtų prie organizacijos „Azure AD“. Be to, gali būti, kad naudotojas atšaukė autentifikavimą.
303	AzureADUserProfile	„HP Sure Admin“ programai nepavyksta gauti naudotojo profilio informacijos iš jūsų organizacijos „Azure AD“.
304	AzureADUserPrincipalMismatch	El. pašto adresas neatitinka prisiregistravusio naudotojo vardo.
305	AzureADUserInvalidUserGroup	Prisiregistravęs naudotojas nepriklauso „Azure AD“ grupei, kuriai priskirtas šis raktas.

4-4 lentelė KMS administratoriaus konsolės klaidos, tipai ir jų aprašai

Klaidos kodas	Klaidos tipas	Aprašas
401	KmsUnauthorized	Naudotojas nėra įgaliotas naudotis KMS paslauga.
402	KmsKeyDoesNotExist	Atitinkančio privataus rakto nėra KMS raktų saugykloje. Raktas šiuo metu panaikintas, tačiau jį galima atkurti, todėl jo pavadinimo šioje būsenoje panaudoti negalima. Dabar raktą galima tik atkurti arba išvalyti.
403	KmsKeyDoesNotExistInTableStorage	Rakto nėra lentelės saugykloje.
404	KmsUploadKeyErrorInKeyVault	Įvyko klaida įtraukiant raktą į raktų saugyklą.
405	KmsUploadKeyUnauthorized	Naudotojas neturi įgaliojimo įkelti raktus. Naudotojas nepriklauso įgaliojimus turinčiai AD grupei, kuri gali kreiptis į šį API.
406	KmsInvalidAzureADLogin	Naudotojas nėra prisijungęs „Azure Tenant AAD“.
407	KmsNoUserGroups	Prisiregistravęs naudotojas nepriklauso jokiai jūsų organizacijos AD grupei.
408	KmsInvalidUserGroup	Prisiregistravęs naudotojas nepriklauso jokiai AD grupei, kuriai yra priskirtas šis raktas.
409	KmsInvalidAccessToken	Užklausoje nurodytas prieigos atpažinimo ženklas yra netinkamas.
410	KmsAccessTokenExpired	Baigėsi pateikto „accessToken“ galiojimo laikas.

4-4 lentelė KMS administratoriaus konsolės klaidos, tipai ir jų aprašai (tęsinys)

Klaidos kodas	Klaidos tipas	Aprašas
411	KmsAccessTokenInvalidTenantId	Pateiktame „accessToken“ yra netinkama „TenantId“ reikšmė.
412	KmsAccessTokenTenantIdMismatch	Pateiktame „accessToken“ nurodyta „TenantId“ reikšmė nesutampa su funkcinės programos „TenantId“.
413	KmsInvalidKeyId	„keyId“ yra nulinis arba tuščias.
414	KmsDeleteKeyUnauthorized	Naudotojas neturi įgaliojimo naikinti raktus. Naudotojas nepriklauso įgaliojimus turinčiai AD grupei, kuri gali kreiptis į šį API.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Bandymas atkurti slaptąjį raktą nepavyko, todėl jo nepavyko atkurti. Naudotojas turėtų bandyti dar kartą.
416	KmsInvalidGetKeysRequest	Užklaus „Gauti raktus“ netinkama.
417	KmsGetKeysUnauthorized	Naudotojas nėra įgaliotas gauti raktų. Naudotojas nepriklauso įgaliojimus turinčiai AD grupei, kuri gali kreiptis į šį API.
418	KmsInvalidRequestPayload	API gauta užklausa netinkama.
419	KmsRequestRequired	Gauta užklausa negali būti tuščia.
420	KmsKeyNotConcurrent	Raktas iš lentelės saugyklos buvo naujintas arba pakeistas po to, kai naudotojas paskutinį kartą gavo kopiją.